A Hierarchy of Quantum Semantics

Simon Perdrix[1]

PPS, University of Paris 7

Abstract

Several domains [1,4,9,12] can be used to define the semantics of quantum programs. Among them Abramsky [1] has introduced a semantics based on probabilistic power domains, whereas the one by Selinger [12] associates with each program a completely positive map. In this abstract, we mainly introduce a semantical domain based on admissible transformations, i.e. multi-sets of linear operators. In order to establish a comparison with existing domains, we introduce a simple quantum imperative language (QIL), equipped with three different denotational semantics, called pure, observable, and admissible. The pure semantics is a natural extension of probabilistic (classical) semantics and is similar to the semantics proposed by Abramsky [1]. The observable semantics, à la Selinger [12], associates with any program a superoperator over density matrices. Finally, we introduce an admissible semantics which associates with any program an admissible transformation. These semantics are not equivalent, but exact abstraction [5] or interpretation relations are established between them, leading to a hierarchy of quantum semantics.

1 Quantum Computing Basics

The basic carrier of information in quantum computing is a 2-level quantum system (*qubit*), or more generally a register of n qubits. The state of a n-qubit register is a normalized vector of a Hilbert space $\mathbb{C}^{2^n}$. So, for a given basis A, a general state $|\varphi\rangle \in \mathbb{C}^{|A|}$ can be written as:

$$\sum_{x\in A} \alpha_x |x\rangle,$$

with $\sum_{x\in A} |\alpha_x|^2 = 1$. Vectors, inner and outer products are expressed in the notation introduced by Dirac. Vectors are denoted $|\varphi\rangle$; the inner product of two vectors $|\varphi\rangle$, $|\psi\rangle$ is denoted by $\langle\varphi|\psi\rangle$. If $|\varphi\rangle = \sum_{x\in A} \alpha_x|x\rangle$ and $|\psi\rangle = \sum_{x\in A} \beta_x|x\rangle$, then $\langle\varphi|\psi\rangle = \sum_{x\in A} \alpha_x^*\beta_x$ (where α^* stands for the complex conjugate). The left hand side $\langle\varphi|$ of the inner product is a *bra-vector*, and the right hand side $|\psi\rangle$ is a *ket-vector*. A bra-vector is defined as the adjoint of the corresponding ket-vector: if $|\varphi\rangle = \sum_{x\in A} \alpha_x|x\rangle$, then $\langle\varphi| = |\varphi\rangle^\dagger = \sum_{x\in A} \alpha_x^*\langle x|$. The bra-ket notation can also be used to describe outer products: $|\varphi\rangle\langle\psi|$ is a linear operator, $(|\varphi\rangle\langle\psi|)|\epsilon\rangle = \langle\psi|\epsilon\rangle\,|\varphi\rangle$. The state of a register composed of 2 sub-systems in state $|\varphi\rangle \in \mathbb{C}^{|A|}$ and $|\psi\rangle \in \mathbb{C}^{|B|}$

[1] Email: simon.perdrix@pps.jussieu.fr

respectively, is the normalized vector $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{C}^{|A|} \otimes \mathbb{C}^{|B|} \cong \mathbb{C}^{|A|\times|B|}$, where $\otimes$ is the tensor product. For any $x \in A, y \in B$, $|x,y\rangle$ denotes $|x\rangle \otimes |y\rangle$.

According to the second postulate of quantum mechanics, an isolated system evolves according to a unitary transformation [2] $U \in \mathbf{L}(\mathbb{C}^{|A|})$, transforming a state $|\varphi\rangle \in \mathbb{C}^{|A|}$ into $U|\varphi\rangle$. A projective measurement is a probabilistic evolution described by a set $\{P_i\}_{\imath\in B}$ of orthogonal projectors [3] which is complete [4]. A measurement produces a classical outcome $i \in B$ and transforms the state $|\varphi\rangle \in \mathbb{C}^{|A|}$ into $\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}$ with probability $\langle\varphi|P_i|\varphi\rangle$.

The composition of two projective measurements is not necessary a projective measurement. However, any any quantum evolution, can be described in a more general framework the *admissible transformations*, which is closed under composition. An admissible transformation is a countable multi-set $\{M_i\}_{i\in A}$ of linear operators which satisfy the completeness condition $\sum_{i\in A} M_i^\dagger M_i = I$. An admissible transformation composed of a unique operator U is an isometry since $U^\dagger U = I$, moreover if $UU^\dagger = I$ then U is a unitary transformation. An admissible transformation composed of projectors only is a projective measurement.

Probability distribution of quantum states of $\mathbb{C}^{|A|}$ can be represented by a density matrix $\rho \in D(\mathbb{C}^{|A|}) \subseteq \mathbf{L}(\mathbb{C}^{|A|})$, i.e. a self adjoint [5] positive-semidefinite [6] complex matrix of trace [7] less than one. A unitary transformation U transforms ρ into $U\rho U^\dagger$ and a projective measurement transforms ρ into $\sum_i P_i\rho P_i$. A projective measurement produces a classical outcome i with probability $Tr(P_i\rho P_i) = Tr(P_i\rho)$.

Any n-qubit unitary transformation U can be approximated within an arbitrary accuracy [8] by composing unitary transformations from the universal set of unitary transformations $\{H, T, CNot\}$, composed of two 1-qubit and one 2-qubit unitary transformations. Notice that there exist several universal families of unitary transformations in the literature [10].

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, CNot = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

2 A Quantum Programming Language

Several quantum programming languages have been introduced recently. For a complete overview see [6] and [11]. In this abstract, we introduce a Quantum Imperative Language (QIL), the syntax is similar to the one of the language introduced

[2] U is unitary if and only if $U^\dagger U = I$.
[3] $\forall i,j \in B, P_iP_j = \delta_{i,j}P_i$ where δ is the Kronecker delta.
[4] $\sum_{i\in B} P_i = I$
[5] M is self adjoint (or Hermitian) if and only if $M^\dagger = M$
[6] M is positive-semidefinite if all the eignenvalues of M are non-negative.
[7] The trace of M ($tr(M)$) is the sum of the diagonal elements of M
[8] U is approximated by V within $\epsilon > 0$ if $||U - V|| < \epsilon$

by Abramsky [1], except for the quantum measurements which are treated implicitly in QIL, like in QML [2].

A QIL program is a pair (Q, C), where $Q = \{q_0, \ldots, q_n\}$ is a finite set of symbols representing a finite memory of qubits, and C is a command defined as follows:

$$\begin{aligned} C ::= \ & \mathsf{skip} \\ & \mid C_1; C_2 \\ & \mid \mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2 \\ & \mid \mathsf{while}\ q\ \mathsf{do}\ C \\ & \mid \mathsf{H}(q) \\ & \mid \mathsf{T}(q) \\ & \mid \mathsf{CNot}(q, q) \end{aligned}$$

Notice that QIL is not limited to a unitary fragment, since according to the semantics of the language, quantum measurements are encoded into the conditional structures of the language: when a qubit q is used as a condition, q is first measured, then the classical outcome of the measurement plays the role of the boolean evaluation of the condition.

Example 2.1

ex1 : while q do $H(q)$	ex2 : while q do $H(q)$;
	H(q) ;
	if q then
	skip
	else
	skip
		ex3 : while q do $H(q)$;
		H(q) ;
		if q then
		H(q)
		else
		H(q)

2.1 A Probabilistic Semantics

According to the postulates of quantum mechanics, the state of a quantum system is a normalized vector in a Hilbert space, and its evolution is probabilistic. Thus, a natural way to define a quantum semantics consists in a quantum version of a classic probabilistic semantics, based for instance on probabilistic power domains [7]. For a given finite set Q, and for any $q \in Q$, let $\mathcal{H}_q = Span(|\mathsf{tt}_q\rangle, |\mathsf{ff}_q\rangle) \cong \mathbb{C}^2$, $\mathcal{H}_Q = \bigotimes_{q \in Q} \mathcal{H}_q \cong \mathbb{C}^{2^{|Q|}}$, and $\mathcal{H}_Q^{\mathbf{1}} = \{|\varphi\rangle \in \mathcal{H}_Q \mid |||\varphi\rangle|| = 1\}$ be the unit sphere of $\mathcal{H}_Q$. $V(\mathcal{H}_Q^{\mathbf{1}})$ is the set of discrete valuations $\nu : \mathcal{H}_Q^{\mathbf{1}} \to \overline{\mathbb{R}^+}$. Let $\mathcal{V}_Q = \{\nu \in V(\mathcal{H}_Q^{\mathbf{1}}) \mid \mathrm{supp}(\nu)$ is discrete and $\sum_{|\varphi\rangle \in \mathrm{supp}(\nu)} \nu(|\varphi\rangle) \leq 1\}$

Theorem 2.2 ([7]) *$(\mathcal{V}_Q, \sqsubseteq)$ is a complete partial order with $\mathbf{0}$ (i.e. the valuation with an empty support) as least element, where $\nu \sqsubseteq \mu$ if and only if $\forall |\varphi\rangle \in \mathrm{supp}(\nu), \nu(|\varphi\rangle) \leq \mu(|\varphi\rangle)$.*

Since any unitary transformation U is reversible, with $U^{-1} = U^\dagger$, the probability that a quantum system is in state $|\varphi\rangle$ after the application of U is equal to the probability that the system was in state $U^\dagger|\varphi\rangle$ before the application of U. Thus, U transforms a discrete valuation ν into $\lambda|\varphi\rangle.\nu(U^\dagger|\varphi\rangle)$.

A projective measurement $\{P_i\}_{i\in B}$, which is not reversible, produces the classical outcome $i \in B$ and transforms a state $|\varphi\rangle$ into $\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}$ with probability $\langle\varphi|P_i|\varphi\rangle$. Thus, $\{P_i\}_{i\in B}$ produces the classical outcome $i \in B$, and transforms a discrete valuation ν into $\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} \nu(|\varphi\rangle)\langle\varphi|P_i|\varphi\rangle\delta_{\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}}$, where $\delta_x(y) = \begin{cases}1 & \text{if } x=y\\ 0 & \text{otherwise}\end{cases}$. Thus, the probability that the classical outcome $i \in B$ occurs is $\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} \nu(|\varphi\rangle)\langle\varphi|P_i|\varphi\rangle$.

Definition 2.3 [Pure semantics] For any finite set Q, for any command C, let $[\![C]\!]_{\mathrm{p}} : \mathcal{V}_Q \to \mathcal{V}_Q$ be defined as follows:

$$
\begin{aligned}
[\![\mathsf{skip}]\!]_{\mathrm{p}} &= I\\
[\![C_1; C_2]\!]_{\mathrm{p}} &= [\![C_2]\!]_{\mathrm{p}} \circ [\![C_1]\!]_{\mathrm{p}}\\
[\![\mathsf{T}(q)]\!]_{\mathrm{p}} &= \lambda\nu.\lambda|\varphi\rangle.\nu(T_q^\dagger|\varphi\rangle)\\
[\![\mathsf{H}(q)]\!]_{\mathrm{p}} &= \lambda\nu.\lambda|\varphi\rangle.\nu(H_q^\dagger|\varphi\rangle)\\
[\![\mathsf{CNot}(q_1,q_2)]\!]_{\mathrm{p}} &= \lambda\nu.\lambda|\varphi\rangle.\nu(CNot_{q_1,q_2}^\dagger|\varphi\rangle)\\
[\![\text{if } q \text{ then } C_1 \text{ else } C_2\ ]\!]_{\mathrm{p}} &= \lambda\nu.[\![C_1]\!]_{\mathrm{p}}\Bigg(\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{tt}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{tt}_q\rangle\langle\mathsf{tt}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{tt}_q\rangle|}}\Bigg)\\
&\quad + [\![C_2]\!]_{\mathrm{p}}\Bigg(\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{ff}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{ff}_q\rangle\langle\mathsf{ff}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{ff}_q\rangle|}}\Bigg)\\
[\![\text{while } q \text{ do } C\ ]\!]_{\mathrm{p}} &= \mathsf{lfp}\Big(\lambda f.\lambda\nu.f\circ[\![C]\!]_{\mathrm{p}}\Bigg(\sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{tt}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{tt}_q\rangle\langle\mathsf{tt}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{tt}_q\rangle|}}\Bigg)\\
&\quad + \sum_{|\varphi\rangle\in\mathrm{supp}(\nu)} |\langle\varphi|\mathsf{ff}_q\rangle|^2\nu(|\varphi\rangle)\delta_{\frac{(|\mathsf{ff}_q\rangle\langle\mathsf{ff}_q|)|\varphi\rangle}{|\langle\varphi|\mathsf{ff}_q\rangle|}}\Big)
\end{aligned}
$$

where M_q means that M is applied on qubit q.
We refer the reader to an extended version of this paper for the technical explainations on continuity and convergence.

Example 2.4 $[\![\mathsf{ex1}]\!]_{\mathrm{p}} = \lambda\nu.\delta_{|\mathsf{ff}\rangle}$, $[\![\mathsf{ex2}]\!]_{\mathrm{p}} = \lambda\nu.(\frac{1}{2}\delta_{|\mathsf{tt}\rangle} + \frac{1}{2}\delta_{|\mathsf{ff}\rangle})$, and $[\![\mathsf{ex3}]\!]_{\mathrm{p}} = \lambda\nu.(\frac{1}{2}\delta_{(|\mathsf{tt}\rangle+|\mathsf{ff}\rangle)/2} + \frac{1}{2}\delta_{(|\mathsf{tt}\rangle-|\mathsf{ff}\rangle)/2)})$

2.2 Observable Semantics

The pure semantics introduced in the previous section does not take into account quantum properties like indistinguishability. For instance, a qubit in state $|\mathsf{tt}\rangle$ or $|\mathsf{ff}\rangle$ with equal probability cannot be distinguished from a qubit in state $\frac{1}{\sqrt{2}}(|\mathsf{tt}\rangle+|\mathsf{ff}\rangle)$ or $\frac{1}{\sqrt{2}}(|\mathsf{tt}\rangle-|\mathsf{ff}\rangle)$ with equal probability. In order to take into account this phenomenon,

one can use the formalism of density matrices (see section 1) to represent quantum states.

For a finite set of variables $Q = \{q_0, \ldots, q_n\}$, let $\mathcal{D}_Q = D(\mathcal{H}_Q)$.

Theorem 2.5 ([12]) *The poset $(\mathcal{D}_Q, \sqsubseteq)$ is a complete partial order with $\mathbf{0}$ as least element, where $M \sqsubseteq N$ if $N - M$ is positive (Löwner partial order).*

Definition 2.6 [Observable semantics] For any finite set Q, for any command C, let $[\![C]\!]_{\mathrm{o}} : \mathcal{D}_Q \to \mathcal{D}_Q$ be defined as follows:

$$\begin{aligned}
[\![\mathsf{skip}]\!]_{\mathrm{o}} &= I \\
[\![C_1; C_2]\!]_{\mathrm{o}} &= [\![C_2]\!]_{\mathrm{o}} \circ [\![C_1]\!]_{\mathrm{o}} \\
[\![\mathsf{H}(q)]\!]_{\mathrm{o}} &= \lambda\rho. H_q \rho H_q^\dagger \\
[\![\mathsf{T}(q)]\!]_{\mathrm{o}} &= \lambda\rho. T_q \rho T_q^\dagger \\
[\![\mathsf{CNot}(q_1, q_2)]\!]_{\mathrm{o}} &= \lambda\rho. CNot_{q_1,q_2} \rho CNot_{q_1,q_2}^\dagger \\
[\![\mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ ]\!]_{\mathrm{o}} &= \lambda\rho. \left([\![C_1]\!]_{\mathrm{o}}(P_q^{\mathsf{tt}} \rho P_q^{\mathsf{tt}}) + [\![C_2]\!]_{\mathrm{o}}(P_q^{\mathsf{ff}} \rho P_q^{\mathsf{ff}}) \right) \\
[\![\mathsf{while}\ q\ \mathsf{do}\ C\ ]\!]_{\mathrm{o}} &= \mathsf{lfp}\left(\lambda f. \lambda\rho. \left(f \circ [\![C]\!]_{\mathrm{o}}(P_q^{\mathsf{tt}} \rho P_q^{\mathsf{tt}}) + P_q^{\mathsf{ff}} \rho P_q^{\mathsf{ff}} \right) \right) \\
&= \lambda\rho. \sum_{n \in \mathbb{N}} (F_{P^{\mathsf{ff}}} \circ ([\![C]\!]_{\mathrm{o}} \circ F_{P^{\mathsf{tt}}})^n(\rho))
\end{aligned}$$

where $P^{\mathsf{tt}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $P^{\mathsf{ff}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $F_M = \lambda\rho. M\rho M^\dagger$.
We refer the reader to an extended version of this paper for the technical explainations on continuity and convergence.

Example 2.7 $[\![\mathsf{ex1}]\!]_{\mathrm{o}} = \lambda\rho. P^{\mathsf{ff}}$, $[\![\mathsf{ex2}]\!]_{\mathrm{o}} = \lambda\rho. \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$, and $[\![\mathsf{ex3}]\!]_{\mathrm{o}} = \lambda\rho. \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$

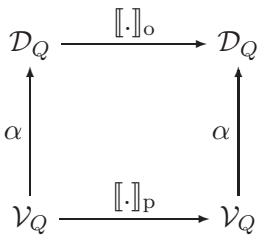
The observable semantics associates with any command C a map $[\![C]\!]_{\mathrm{o}}$. $[\![C]\!]_{\mathrm{o}}$ is a superoperator[9], thus for any $\rho \in \mathcal{D}_Q$, $[\![C]\!]_{\mathrm{o}}(\rho) \in \mathcal{D}_Q$.

Observable and probabilistic semantics of QIL are not equivalent, as it is illustrated in example 2.4 and 2.7: $[\![\mathsf{ex2}]\!]_{\mathrm{o}} = [\![\mathsf{ex3}]\!]_{\mathrm{o}}$ whereas $[\![\mathsf{ex2}]\!]_{\mathrm{p}} \neq [\![\mathsf{ex3}]\!]_{\mathrm{p}}$. However, observable semantics is an exact abstraction [5] of the probabilistic semantics. Any probability distribution over quantum states ν can be abstracted into a density matrix $\rho = \alpha(\nu)$, where $\alpha : \mathcal{V}_Q \to \mathcal{D}_Q$ is defined as $\alpha = \lambda\nu. \sum_{|\varphi\rangle \in supp(\nu)} \nu(|\varphi\rangle)\, |\varphi\rangle\langle\varphi|$.

Lemma 2.8 $[\![.]\!]_{\mathrm{o}}$ *is an α-abstraction of $[\![.]\!]_{\mathrm{p}}$, i.e. for any command C,*

$$[\![C]\!]_{\mathrm{o}} \circ \alpha = \alpha \circ [\![C]\!]_{\mathrm{p}}$$

[9] F is a superoperator if $F(\rho)$ is positive whenever ρ is positive, and $Tr(F(\rho)) \leq Tr(\rho)$.



Lemma 2.8 establishes a connection between two domains used in quantum computation. Observable and pure semantics are not equivalent, however the observable semantics is an abstraction of the pure one. This abstraction carries the indistinguishability to the pure semantics: let C_1 and C_2 two commands such that $[\![C_1]\!]_{\mathrm{p}} \neq [\![C_2]\!]_{\mathrm{p}}$ and $[\![C_1]\!]_{\mathrm{o}} = [\![C_2]\!]_{\mathrm{o}}$, then for any $\nu \in \mathcal{V}_Q$, $[\![C_1]\!]_{\mathrm{p}}(\nu)$ and $[\![C_1]\!]_{\mathrm{p}}(\nu)$ are indistinguishable. However, even if observable and pure semantics are not equivalent, none of them violate the postulates of quantum mechanics. Notice that the author have established a similar exact abstract connection for the semantics of the quantum calculus [8].

Additionally to the abstraction function $\alpha : \mathcal{V}_Q \to \mathcal{D}_Q$, a concretization function $\gamma : \mathcal{D}_Q \to \mathcal{V}_Q$ is defined as follows: for any $\rho \in \mathcal{D}_Q$, if $\rho = \sum_{i\in A} \lambda_i |\varphi_i\rangle\langle\varphi_i|$ is the spectral decomposition of ρ, then $\mathrm{supp}(\gamma(\rho)) = \{|\varphi_i\rangle\}_{i\in A}$, and $\forall i \in A$, $\gamma(\rho)(|\varphi_i\rangle) = \lambda_i$. For any command C, since $\alpha \circ \gamma = I$, the exact abstract of lemma 2.8 can be stated as:

$$[\![C]\!]_{\mathrm{o}} = \alpha \circ [\![C]\!]_{\mathrm{p}} \circ \gamma$$

2.3 Admissible semantics

According to the postulates of quantum mechanics, any quantum evolution can be described by an admissible transformation, i.e. a countable multi-set of linear operators (see section 1). In this section, we introduce a denotational semantics associating with every program an admissible semantics.

Let $\mathcal{M}_Q$ be the set of all countable multi-sets $\{M_i\}_{i\in A}$ such that $\forall i \in A, M_i \in \mathbf{L}(\mathcal{H}_Q)$ and $\sum_{i\in A} M_i^\dagger M_i \sqsubseteq I$. Let $m_K(x)$ be the multiplicity of x in the multi-set K, i.e. the number of occurrences of x in K. The join $K \uplus L$ of two multi-sets K, L is such that for any x, $m_{K\uplus L}(x) = m_K(x) + m_L(x)$. Moreover, composition $\bullet$ of admissible transformations is defined as follows: for any $(M_i)_{i\in A}, (M'_j)_{j\in B} \in \mathcal{M}_Q$, $(M_i)_{i\in A} \bullet (M'_j)_{j\in B} = (M_i M'_j)_{(i,j)\in A\times B}$.

Theorem 2.9 *$(\mathcal{M}_Q, \subseteq)$ is a complete partial order with $\{0\}$ as least element.*

Definition 2.10 [Admissible semantics] For any finite set Q, for any command C, let $[\![C]\!]_{\mathrm{p}} : \mathcal{M}_Q \to \mathcal{M}_Q$ be defined as follows:

$$\begin{aligned}
[\![\mathsf{skip}]\!]_{\mathrm{a}} &= \{I\}\\
[\![C_1;C_2]\!]_{\mathrm{a}} &= [\![C_2]\!]_{\mathrm{a}} \bullet [\![C_1]\!]_{\mathrm{a}}\\
[\![\mathsf{H}(q)]\!]_{\mathrm{a}} &= \{H_q\}\\
[\![\mathsf{T}(q)]\!]_{\mathrm{a}} &= \{T_q\}\\
[\![\mathsf{CNot}(q_1,q_2)]\!]_{\mathrm{a}} &= \{CNot_{q_1,q_2}\}\\
[\![\mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ ]\!]_{\mathrm{a}} &= \left([\![C_1]\!]_{\mathrm{a}} \bullet \{P_q^{\mathsf{tt}}\}\right) \uplus \left([\![C_2]\!]_{\mathrm{a}} \bullet \{P_q^{\mathsf{ff}}\}\right)\\
[\![\mathsf{while}\ q\ \mathsf{do}\ C\ ]\!]_{\mathrm{a}} &= \biguplus_{k=0}^{\infty} \left(\{P_q^{\mathsf{ff}}\} \bullet ([\![C]\!]_{\mathrm{a}} \bullet \{P_q^{\mathsf{tt}}\})^n\right)
\end{aligned}$$

We refer the reader to an extended version of this paper for the technical explainations on continuity and convergence.

Example 2.11 $[\![\mathsf{ex1}]\!]_{\mathrm{a}} = \{\begin{pmatrix} 0 & 0\\ 0 & 1\end{pmatrix}\} \uplus \{\begin{pmatrix} 0 & 0\\ \frac{1}{(n+2)^2} & 0\end{pmatrix}\}_{n\in\mathbb{N}}$

$[\![\mathsf{ex2}]\!]_{\mathrm{a}} = \{\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0\\ 0 & -1\end{pmatrix}\} \uplus \{\frac{1}{\sqrt{2}}\begin{pmatrix} \frac{1}{(n+2)^2} & 0\\ 0 & 0\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0\\ \frac{-1}{(n+2)^2} & 0\end{pmatrix}\}_{n\in\mathbb{N}}$

$[\![\mathsf{ex3}]\!]_{\mathrm{a}} = \{\frac{1}{2}\begin{pmatrix} 0 & 1\\ 0 & 1\end{pmatrix}, \frac{1}{2}\begin{pmatrix} 0 & -1\\ 0 & 1\end{pmatrix}\} \uplus \{\frac{1}{2}\begin{pmatrix} \frac{1}{(n+2)^2} & 0\\ \frac{1}{(n+2)^2} & 0\end{pmatrix}, \frac{1}{2}\begin{pmatrix} \frac{-1}{(n+2)^2} & 0\\ \frac{1}{(n+2)^2} & 0\end{pmatrix}\}_{n\in\mathbb{N}}$

Admissible transformations and superoperators are related by the Krauss representation theorem [3]: for any superoperator F, there exists a set of linear operators $\{M_i\}_{i\in A}$ such that $F = \lambda\rho.\sum_{i\in A} M_i\rho M_i^\dagger$. Notice that this set of linear operators is not unique. Any admissible transformation can be seen as the representation of a superoperator. $\chi_{\mathrm{o}} : \mathcal{M}_Q \to (\mathcal{D}_Q \to \mathcal{D}_Q)$ is an interpretation function which associates with any admissible transformation $\{M_i\}_{i\in A}$ a superoperator $\chi_{\mathrm{o}}(\{M_i\}_{i\in A}) = \lambda\rho.\sum_{i\in A} M_i\rho M_i^\dagger$. The observable semantics is an interpretation of the admissible semantics:

Lemma 2.12 *For any command C, $[\![C]\!]_{\mathrm{o}} = \chi_{\mathrm{o}}([\![C]\!]_{\mathrm{a}})$.*

Moreover, admissible transformations can also be interpreted in terms of probabilistic evolutions via the function $\chi_{\mathrm{p}} : \mathcal{M}_Q \to (\mathcal{V}_Q \to \mathcal{V}_Q)$ which associates with any admissible transformation $\{M_i\}_{i\in A}$ a probabilistic evolution $\chi_{\mathrm{p}}(\{M_i\}_{i\in A}) = \lambda\nu.\sum_{i\in A,|\varphi\rangle\in\mathrm{supp}(\nu)} \nu(|\varphi\rangle)\langle\varphi|M_i^\dagger M_i|\varphi\rangle\delta_{\frac{M_i|\varphi\rangle}{\sqrt{\langle\varphi|M_i^\dagger M_i|\varphi\rangle}}}$. The pure semantics is an interpretation of the admissible semantics:

Lemma 2.13 *For any command C, $[\![C]\!]_{\mathrm{p}} = \chi_{\mathrm{p}}([\![C]\!]_{\mathrm{a}})$.*

Notice that lemma 2.12 can be seen as a consequence of lemmas 2.8 and 2.13: for any command C, $[\![C]\!]_{\mathrm{o}} = \alpha\circ[\![C]\!]_{\mathrm{p}}\circ\gamma$ and $[\![C]\!]_{\mathrm{p}} = \chi_{\mathrm{p}}([\![C]\!]_{\mathrm{a}})$, so $[\![C]\!]_{\mathrm{o}} = \alpha\circ\chi_{\mathrm{p}}([\![C]\!]_{\mathrm{a}})\circ\gamma$.

The admissible semantics associates with any program an admissible transformation. Since an admissible transformation is not a function but a multi-set of linear operators, no connection based on abstraction function can be realized with

the pure and observable semantics introduced in previous sections. However, interpretation functions, χ_{p} and χ_{o} transform the admissible semantics into the pure and the observable semantics, showing that the admissible semantics is a more concrete semantics. Since admissible semantics is more concrete than pure semantics, the indistinguishability phenomenon is not taken into account as it is illustrated in example 2.11, since $[\![\mathsf{ex2}]\!]_{\mathrm{a}} \neq [\![\mathsf{ex2}]\!]_{\mathrm{a}}$. In order to illustrate the concreteness of the admissible semantics, one can notice in the definition of the semantics that the existence of while loop in a command C implies that the admissible semantics of C is an infinite multi-set: each linear operator of the admissible transformation represents a computational path.

Exact abstraction and interpretations between the semantics established in lemmas 2.8, 2.12, and 2.13 lead to a semantical hierarchy:

Theorem 2.14 (Hierarchy of quantum semantics) *For any commands* C_1, C_2,

$$[\![C_1]\!]_{\mathrm{a}} = [\![C_2]\!]_{\mathrm{a}} \implies [\![C_1]\!]_{\mathrm{p}} = [\![C_2]\!]_{\mathrm{p}} \quad \textit{and} \quad [\![C_1]\!]_{\mathrm{p}} = [\![C_2]\!]_{\mathrm{p}} \implies [\![C_1]\!]_{\mathrm{o}} = [\![C_2]\!]_{\mathrm{o}}$$

3 Conclusion

We have mainly proved that the semantics of a quantum program can be based on admissible transformations, i.e. multi-sets of linear operators. We have introduced a complete partial order over admissible transformations and defined an admissible semantics, based on admissible transformations, of a simple quantum imperative language (QIL). In order to compare with existing technics, two additional semantics based on probability distributions over pure states (pure semantics) and on density matrices (observable semantics) are defined. This three semantics are not equivalent and leads to a hierarchy where the admissible semanitics is the most concrete one. The pure semantics, based on probabilistic power domain is more abstract, whereas the most abstract semantics is the one based on density matrices.

References

[1] S. Abramsky. A Cook's tour of a simple quantum programming language. *3rd International Symposium on Domain Theory, Xi'an, China*, May 2004.

[2] Thorsten Altenkirch and J. Grattage. QML: Quantum data and control. Manuscript, 2005.

[3] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, 10:285, 1975.

[4] Bob Coecke and Keye Martin. A partial order on classical and quantum states. Technical report, PRG-RR-02-07, 2002.

[5] P. Cousot. Types as abstract interpretations. In *POPL*, pages 316–331, 1997.

[6] S. J. Gay. Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science*, 16(4), 2006.

[7] C. Jones and G. D. Plotkin. A probabilistic powerdomain of evaluations. In *LICS*, pages 186–195, 1989.

[8] Ph. Jorrand and S. Perdrix. Towards a quantum calculus. In *To appear in Proceedings of the 4th International Workshop on Quantum Programming Languages, ENTCS*, 2006.

[9] E. Kashefi. Quantum domain theory — definitions and applications. In *Proceedings of the International Conference on Computability and Compexity in Analysis*, number 302 – 8/2003 in Fernuniversität Hagen Informatik Berichte, 2003.

[10] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[11] P. Selinger. A brief survey of quantum programming languages. In *Proceedings of the 7th International Symposium on Functional and Logic Programming*, volume 2998 of *Lecture Notes in Computer Science*, pages 1–6. Springer, 2004.

[12] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.